UNIVERSIDADE DE LISBOA
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE INFORMÁTICA

PREVENTING DOS ATTACKS IN MULTI-DOMAIN OPTICAL SDN

Nuno Filipe Gomes Ferreira

MESTRADO EM SEGURANÇA INFORMÁTICA
Versão pública

Dissertação orientada por:
Prof. Doutor Fernando Ramos
Eng. David Silva

2016

Agradecimentos

A realização deste trabalho teve muitos apoios e incentivos de diversas pessoas. Todos os contributos foram essenciais para o desenvolvimento e realização do mesmo. Desta forma, gostaria de agradecer e mostrar o meu apreço a todos os que me ajudaram e acompanharam ao longo deste percurso.

Ao professor Doutor Fernando Ramos pela orientação e disponibilidade que demonstrou ao longo da realização deste projeto.

Ao meu coorientador David Silva pela disponibilidade e acompanhamento na realização da parte prática deste projeto.

À engenheira Paula Gestal, que sempre me incentivou e me deu as condições necessárias para que concluísse o mestrado.

Aos meus colegas do mestrado e da empresa onde colaboro, pela amizade e companheirismo que me proporcionaram ao longo de todo o mestrado.

Por último, à minha familia e amigos por todo o apoio, carinho e motivação que me deram ao longo do mestrado.

A todos um muito obrigado por tornarem possível a conclusão de mais uma etapa da minha vida.

Resumo

As redes tradicionais começam a não ter o dinamismo necessário para acompanhar a evolução que os serviços *on-line* têm vindo a ter nos últimos anos. Como forma de contornar este problema, foi proposto recentemente um novo paradigma de redes: *Software Defined Networking* (SDN). Enquanto nas redes tradicionais o plano de controlo se encontra junto do plano de dados, isto é, o equipamento de rede é responsável não só por encaminhar pacotes (plano de dados), mas também por decidir como encaminhar o tráfego (plano de controlo), em SDN estas duas camadas são separadas. Em SDN é utilizado um controlador logicamente centralizado para controlar toda a rede. Com esta separação, uma SDN traz vários benefícios que estão relacionados com a programabilidade introduzida pelo controlador e com a visão geral que este possui de toda a rede.

Para se poder beneficiar deste novo paradigma, é necessário que exista um plano de migração dos vários tipos de redes existentes. Na arquitetura SDN, como o plano de controlo é implementado num controlador logicamente centralizado, é necessário que este comunique com os equipamentos do plano de dados através de uma *interface standard* que abstraia os detalhes de implementação específicos do *hardware* dos equipamentos. Para as redes de comutação de pacotes o protocolo *OpenFlow* fornece essa *interface standard* para o *hardware*, facilitando a sua migração. No caso das redes ópticas a passagem para o paradigma SDN não será simples devido ao facto dos equipamentos ópticos suportarem diferentes protocolos de comunicação e não existirem interfaces *standard* SDN preparadas para o seu suporte.

Para os provedores de serviços de telecomunicações, esta evolução é um desafio, pois requer o desenvolvimento de toda a infraestrutura para controlar e gerir os equipamentos ópticos. Para estes o ideal seria manter a gestão e o controlo do lado dos fornecedores de equipamentos ópticos, e gerir e controlar os equipamentos ópticos de diferentes fornecedores (redes ópticas multidomínio) de uma forma unificada. Desta forma, vários provedores de serviços: China Mobile, China Telecom, Verizon e organizações da indústria como o *Open Networking Foundation* (ONF) propuseram a criação de uma camada de abstração entre o controlador dos provedores de serviços e os equipamentos ópticos. Essa camada de abstração será responsável por converter a linguagem dos equipamentos ópticos numa *Application Programming Interface* (API) *standard* SDN para comunicação com o controlador principal. Cada vendedor de equipamentos ópticos será responsável por fornecer os equipamentos ópticos e a respetiva camada de abstração. Podemos considerar esta camada de abstração como sendo um controlador de equipa-

mentos ópticos: o controlador *Original Equipment Manufacturer* (OEM). Desta forma, os provedores de serviços apenas terão de arranjar um controlador localizado na camada superior da hierarquia que seria responsável por orquestrar toda rede, utilizando para isso a abstração fornecida pelos controladores de equipamentos ópticos. É de notar que o controlo e a gestão dos equipamentos ópticos não é feita diretamente pelo controlador dos provedores de serviços, mas sim na camada de abstração abaixo, ou seja, pelos controladores de equipamentos ópticos. Com esta abordagem, os provedores de serviços ficam sem o controlo completo do sistema, pois ficam dependentes das operações e da informação que é dada pelos controladores de equipamentos ópticos, como por exemplo informação de desempenho dos serviços, alarmes ou estados da rede óptica. Neste contexto, como poderão os fornecedores de equipamentos ópticos dar garantias de segurança aos provedores de serviços? Se a disponibilidade ou a integridade do controlador dos equipamentos ópticos for comprometida, poderá haver negação de serviço (o controlador de equipamentos ópticos deixaria de processar informações importantes da rede óptica, como por exemplo alarmes) ou quebras de tráfego (desativação de serviços ópticos), o que seria indesejável e poderia trazer avultados prejuízos para os provedores de serviços. Nesta tese a principal motivação é de facto garantir que o controlador de equipamentos ópticos mantém a sua disponibilidade e integridade no processamento de todos os pedidos.

O objetivo deste trabalho é assim desenvolver uma solução que proteja os controladores de equipamentos ópticos de eventuais ataques de negação de serviço. É de notar que mesmo havendo protecção nos *links* ópticos, um utilizador malicioso poderá colocar o controlador de equipamentos ópticos indisponível, bloqueando assim o acesso à rede óptica por parte do provedor de serviços (se houver problemas na rede óptica, estes não serão detetados). A solução que propomos para este problema é a implementação de mecanismos de monitorização e análise dos pedidos ao controlador de modo a controlar o fluxo de dados à entrada do controlador de equipamentos ópticos e assim garantir a sua disponibilidade. Esta protecção será feita através da utilização de uma *reverse proxy* e de uma firewall. Para além destes dois mecanismos de protecção, a comunicação entre o controlador do provedor de serviços e o controlador de equipamentos ópticos é feita de forma segura, de modo a garantir a integridade de todos os pedidos.

Palavras chave: Software defined networking, equipamentos ópticos, provedores de serviços, controladores de equipamentos ópticos, segurança, monitorização, disponibilidade, integridade.

Abstract

Legacy networks do not have the necessary dynamism to follow the evolution online services have experienced in the past few years. In order to overcome this problem, the Software Defined Networking (SDN) paradigm was proposed. The goal of this paradigm is change the way networks are controlled. In legacy networks, the control plane and the data plane are coupled together in the network elements. SDN separates the control plane and the data plane through the use of a standard SDN Application Programming Interface (API) in the data plane to communicate with the logically centralized control plane. In order to reap the benefits of SDN, a plan of migration for legacy networks should be established. For optical networks the migration to SDN is not easy because optical equipments have their own protocols to communicate and there are no SDN standardized interfaces prepared to abstract these type of equipments. In order to solve this problem, organizations such as China Mobile, China Telecom, Verizon and industry organizations like the Open Networking Foundation (ONF) have proposed the use of an abstraction layer between the data plane and the main controller. This abstraction layer is responsible to convert the optical equipment protocols into a standard SDN Application Programming Interface (API) to communicate with the main controller. The abstraction layer can be considered an optical equipment controller, the Original Equipment Manufacturer (OEM) controller. With this approach, service providers (SP) (i.e., telecommunication operators) only need to have a main controller to orchestrate the whole network through the use of OEM controllers. With this solution the Service Providers (SP) are able to control the optical network with different optical equipment from multiple vendors (multi-domain networks).

The OEM controllers are responsible to execute all the operations in the Network Element (NE) (the NE is the optical equipment) that constitutes the Data Plane (DP). They also process information that comes from the NE and translate that information to the main controller. Examples include: network information and performance of services. The challenge is that if the OEM controller is compromised, the entire optical network is compromised. This is the main motivation for this project.

The objective of our work is to develop a solution that can help the Service Provider (SP) to have confidence in the NEs and respective optical network connections. To achieve this goal, the system has to guarantee the availability of the OEM controller. The integrity of the communication between the SP orchestrator and the OEM controller should also be guaranteed. The OEM controller should be always available to process notifications, be it from the

NEs or from the main controller. It should also be ensured that the integrity of all requests that are sent by the SP controller to the OEM controllers is guaranteed.

In order to solve these problems, we propose a new security mechanism for the OEM controller to protect the optical network. The solution consists in the use of a reverse proxy and a firewall to control the flow of requests to the OEM controller. The communication between the SP controller and the OEM controller is also made secure to assure the integrity of requests.

Key words: Software defined networking, optical network equipment, service providers, OEM controllers, security, monitoring, availability, integrity, Network Elements.

Contents

List of Figures

List of acronyms

API Application Programming Interface

ASON Automatically Switched Optical Network

CP Control Plane

DWDM Dense Wavelength Division Multiplexing

DP Data Plane

DoS Denial-of-Service

EDM Evolving Defence Mechanism

EMS Element Management System

GMPLS Generalized Multi Protocol Label Switching

ICMP Internet Control Message Protocols

IM Interface Manager

IP Internet Protocol

MP Management Plane

NDM Network Domain Manager

NE Network Element

NMS Network Management System

OAMD Optical Add Drop Multiplexer

OEM Original Equipment Manufacturer

OIF Open Interface Forum

OLR Optical Line Repeater

OMD Optical Multiplexer / Demultiplexer

ONF Open Networking Foundation

OSI Open System Interconnection

OTN Optical Transport Network

PCE Path Computation Element

ROADM Reconfigurable optical add and drop multiplexing

SDN *Software Defined Networking*

SLA Service Level Agreement

SLAM Service Level Agreement Manager

SP Service Provider

SPAP Service Provider Administration Portal

STRIDE Spoofing identity; Tampering with data; Repudiation; Information disclosure; Denial of service; Elevation of privilege

TLS Transport Layer Security

WDM Wavelength Division Multiplexing

WSS Wavelength Selective Switching

Chapter 1

Introduction

1.1 Legacy optical networks

The society depends on information access. Today, most things are connected, and information is accessible from almost anywhere. That brings new challenges to network management and control. To cope, networks need to be more dynamic and allow better and efficient control. Most networks are managed and controlled by Service Providers (SP) or carriers. These networks are used to provide a variety of services to their costumers [21]. Delivering these services requires guarantees of high throughput from the network, and for that reason optical networks now form the core of SP networks.

Optical networks use optical fibers, whose characteristics provide more bandwidth than copper cables and make them less susceptible to various kinds of electromagnetic interferences [21]. These networks are composed of optical equipments that are deployed in Network Elements (NE)s. Each NE consists in a group of shelfs where the optical cards are placed and interconnected. An example of an NE can be seen in Figure 1.1. In this figure it is possible to see a shelf with several cards and the optical ports of each card used to connect the fibers. NE equipment is sold by optical vendors. A SP typically uses optical equipment from multiple vendors (multivendor networks).

In Figure 1.2 we illustrate how a large terrestrial network is segmented. The SP telecommunication network is typically organized into metropolitan (metro) areas. Each of these areas are interconnected by the core network using optical fibers [8].

In optical networks, each NE is managed individually through the use of vendor-specific interfaces, and that requires highly skilled personnel to make

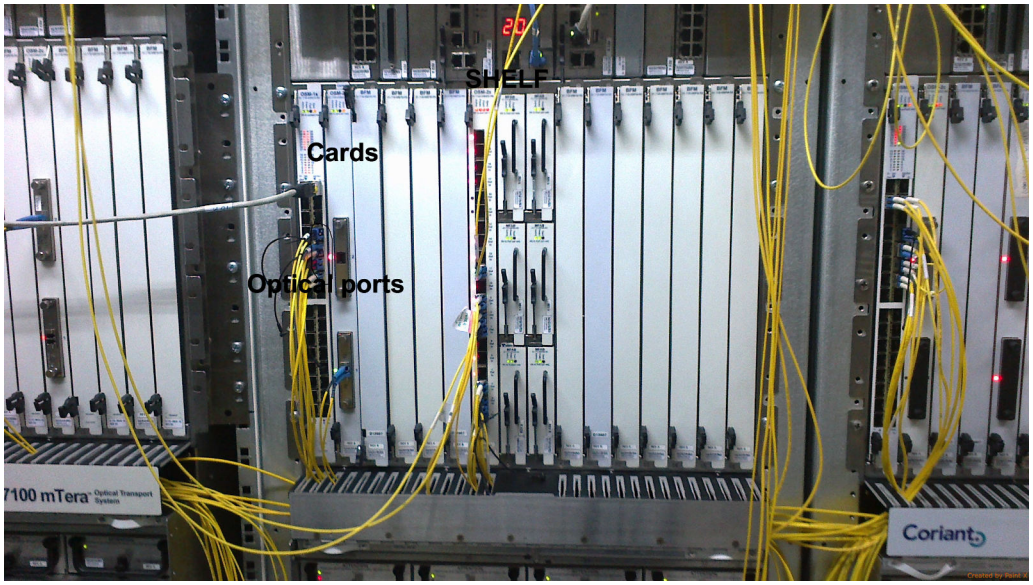

Figure 1.1: Network Element.

the proper configurations. This creates an increase in operational costs, since the provisioning and management of large multivendor networks became extremely expensive [25]. However, the income for operations has been decreasing over the last years. As such, the SP has interest in solutions that can merge optical network management and provisioning across multivendor networks in order to reduce costs, simplify management, improve provisioning time and improve resource utilization [11]. Also, the vertical integration of these networks (the control plane and data plane are coupled together inside the network devices), reduces the flexibility, innovation and evolution of the network infrastructure [15]. A new networking paradigm that tries to solve the previous problems is Software Defined Networking (SDN).

1.1.1 Legacy optical networks versus SDN

The main difference between traditional or legacy optical networks and SDN can be seen in figure 1.3. Networks are composed by a Management Plane (MP), a Control Plane (CP) and a Data Plane (DP). The MP corresponds to the function applications that are responsible to implement network management and operations logic [15]. In optical networks this plane is responsible to manage the optical equipment through the use of a Network Management System (NMS) or Element Management System (EMS). The CP is the component that defines how traffic is handled. Finally, the DP corresponds

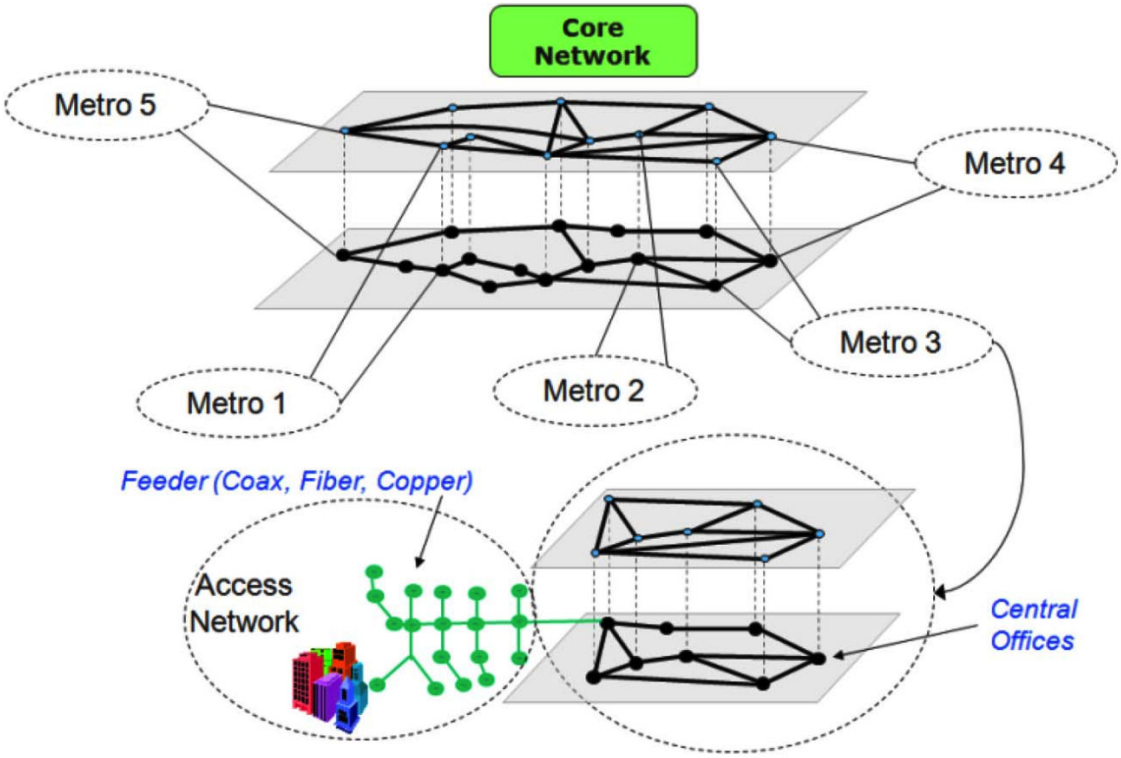

Figure 1.2: Terrestrial network layer and segmentation. Figure from [8]

to the place where the optical devices are interconnected. In legacy optical networks, the CP and DP are coupled together inside the network equipment.

SDN decouples the CP and the DP. For this purpose it uses a well defined southbound interface to communicate with the NEs in the DP. The communication is done through the use of a standard Application Programming Interface (API), such as OpenFlow [15]. With this separation, the CP can be seen as the network brain of the SDN architecture. This separation brings several advantages over legacy optical networks [15]: First, the programmability of applications is simplified since it provides an abstraction layer (the CP). Second, the logically centralized CP gives a global view of the network, which can be used to make effective and consistent decisions in the network. Third, applications are able to take actions from any part of the network (this includes automatic reconfigurations when necessary). Fourth, the integration of more devices in the network is simplified and more straightforward. All these advantages are very important to improve optical

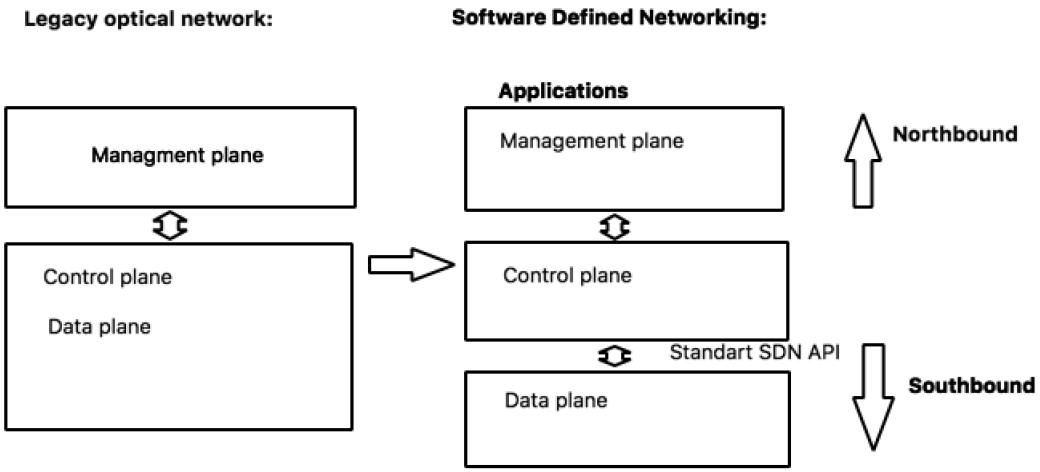

Figure 1.3: Legacy optical networks vs SDN

network management and control, specially in multivendor scenarios.

1.1.2 Migration of legacy optical networks to SDN

In order to benefit from the SDN architecture, an effective migration plan from legacy optical networks is necessary. In SDN, the control plane is implemented in a logically centralized [1] controller that communicates with the data plane through the use of a standardized interface that abstracts hardware-specific implementation details. OpenFlow is the protocol that provides a standardized interface to packet based networks. Unfortunately, it does not yet provide the same mechanisms for optical networks. The migration of optical networks to SDN is not simple [11] because in these networks the NEs have their own protocols to communicate and there are no standardized interfaces prepared to abstract different optical equipment. In order to benefit from the SDN capabilities in optical networks, some improvements are further needed to achieve the necessary flexibility at the photonics and electrical layers [19].

As stated above, optical networks can be managed through the use of a NMS or an EMS. These two management interfaces belong to the management plane. The EMS is used to manage each NE individually. The NMS is an application that is used to manage the optical network from a specific

[1] By logically centralized we mean the automation can be implemented as a distributed system [14]

optical vendor. Each optical vendor use a different NMS that is adapted to their optical equipment. In the NMS, the management requires network operators to design circuits (the configurations in the optical equipment should match with the hardware) and consequently drive the configuration of NEs.

Another requirement that need to be fulfilled by a migration plan is, for the service providers, the optical network to be resilient in order to ensure the desired level of survivability, to fulfill the Service Level Agreement (SLA) [8]. Normally the service availability is defined within this SLA, and that means for example that an availability value of 99.999% can tolerate an outage of 5 min per year. In order to achieve this, the SPs have to use protection links in the optical layer and recovery mechanisms.

Optical resilience can be divided to two main fields: multilayer resilience and multi-domain resilience [8]. Multilayer resilience is illustrated in Figure 1.4. The idea is to take the advantage of recovery options on different technology layers that compose the Open System Interconnection (OSI) model. In this figure, the NEs compose the optical layer and all traffic will flow on this layer (it represents the layer 1 of OSI model). In the upper layers, appear the Client layers of the optical layer. This means if one link fails in the optical layer, for instance, the services that are running in client layer will be notified and then will change to an available connection in the optical layer. For example, if the link four in the Figure fails, the connection between B and C will change to B-E-C.

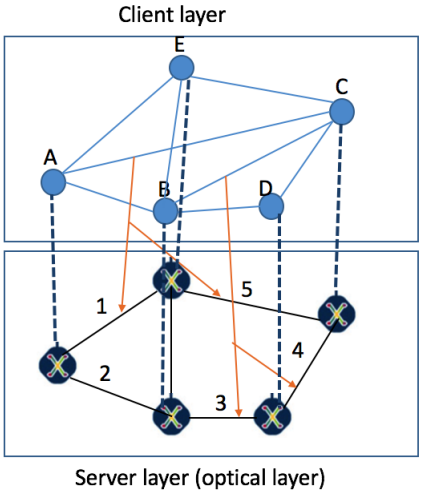

Figure 1.4: Example of Multilayer Resilience

Several improvements have been implemented to make these (multilayer)

networks more autonomous. Several operators have adopted the Automatically Switched Optical Network (ASON) architecture using the Generalized Multi Protocol Label Switching (GMPLS) [17] protocol as their optical transport control plane. The GMPLS has been standardized [17] to facilitate the automated control of multilayer networks. For this purpose, it uses routing and signaling protocols to facilitate dynamic service setup, to provide capacity or to protect services through the use of recovery options on different technology layers [23]. The main problem is the compatibility of optical equipment to support this type of resilience.

The second type of optical resilience is multi-domain. Multi-domain resilience is shown in Figure 1.5. Basically each domain is composed by equipment from one optical vendor (Coriant, Huawei, Alcatel..), and that makes the interoperability between domains a hard task. In this case, the objective is to provide end-to-end service resilience over multiple network domains (also called multivendor networks). Here, sharing information between domains is a critical point.

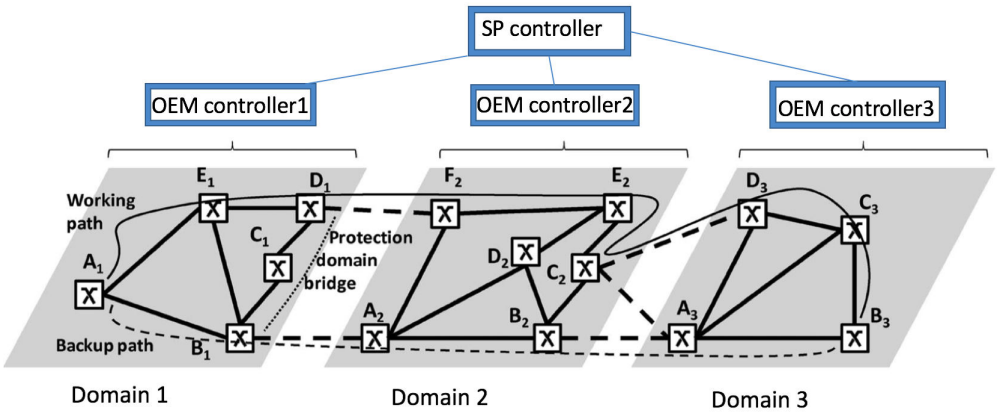

Figure 1.5: Multi-domain Resilience (from [23])

As can be observed in figure 1.5, each domain has a Original Equipment Manufacturer (OEM) controller that is used to compute end-to-end paths by standardized interfaces between layers in a specific domain. The OEM controller is only able to communicate with NEs in a specific domain. In order to have resilience in a path from Domain 1 to Domain 3, for instance it is necessary to introduce a higher controller that has global information on domains. This is the place where an SDN approach could bring benefits. With SDN it will be possible to control and manage paths that cross several domains.

To manage and control optical paths that traverse several domains, several techniques have been proposed: [20], [5], [4]. Basically all these solutions are based on the use of an hardware abstraction layer. They use this intermediate layer between the NEs and the main controller (SP controller) for communication via southbound, and in the northbound a standard SDN API (Restconf, OpenFlow or other) is used to communicate with the main controller (in this case the SP controller). With this approach, a service provider can manage and control the entire network even though optical equipment from different providers is used (each optical network vendor will use its own abstraction layer). In order to make this possible, Service Providers like China Mobile [29], China Telecom [9], Verizon [10] and industry organizations like Open Networking Foundation (ONF) [22] have proposed an architecture where the Original Equipment Manufacturer (OEM) domain controllers will manage the optical NEs within each vendor's own domain while providing open northbound interfaces to a common network orchestrator (a parent "super" controller), as in Figure 1.6. In this figure it can be seen that each optical network (1,2..n) is managed through the use of a specific OEM controller. The SP controls the common network orchestrator that is used to manage and control the whole network. From the SDN point of view, the data plane is represented by the NEs in the optical network. The main diference here is the control plane. In this scenario, the control plane is composed by the OEM controllers and by the common network orchestrator. As such, the control is split between the SP controller and the OEM controllers. The SP controller will have the vision and control of the global network throw the use of OEM controllers. With this approach we achieve control and management over optical networks in a multi-domain optical SDN environment.

One of the main challenges of these networks is security. In the next section we will give a security overview of standard SDN and multi-domain optical SDN networks.

1.2 Security in multi-domain optical SDN environments

The standard SDN architecture is different from a multi-domain optical SDN environment architecture in that, the data plane equipment in the latter is not SDN compatible. As such, different techniques need to be put in place to secure this new environment.

Several security surveys [24], [1], [3] have given an overview of security in

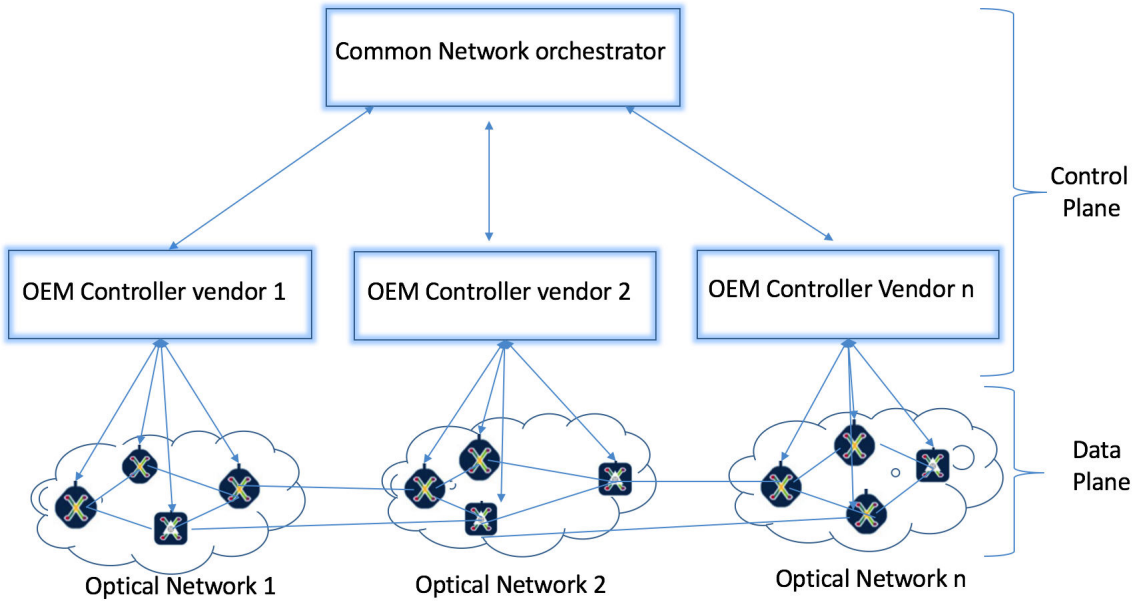

Figure 1.6: Optical network management and control in an SDN environment.

standard SDN. These surveys are adapted to the case where the equipment's in the data plane are compatible with an SDN API. That is not the case when we have several OEM controllers managing different NEs, with a main controller orchestrating the network globally. In this case, more layers, interfaces (with respect to the OEM controller) appear and the security analysis became more complex.

Regarding security, standard SDN brings several benefits. The separation of the control plane and data plane gives SDN an enhancement in security by means of global network visibility. Any conflicts that appear in the network can be more easily solved by the logically centralized control plane. However, this change also brings new security problems. New threats [24], [1] appear as a result of this separation. This new threats are mainly related to man-in-the-middle attacks and Denial of service (DoS) attacks.

With the additional division of control brought by using a two-tier hierarchy of SDN controllers, in multi-domain optical networks, new security problems may arise. For example, a man-in-the-middle attack can be performed to change the information that is sent from the SP controller to the OEM controller. In this case, the integrity of the request will be at risk. This problem can be solved with the use of Transport Layer Security (TLS) in the

communications between these two components. DoS attacks are also possible. Basically, in this case a DoS attack can be done to the main controller, to the OEM controllers or to the optical equipment. A DoS attack to any controller can put the resilience of the entire optical network at risk.

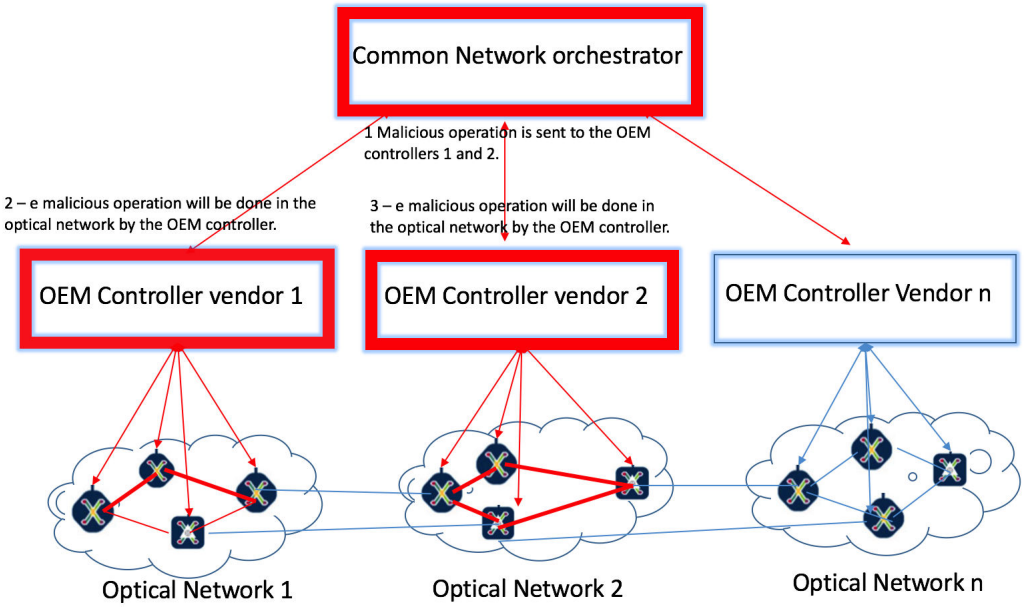

Figure 1.7: Example of a possible attack to the optical network.

If a malicious user intercepts the traffic between the OEM controller and the common network orchestrator it will be able to make fake requests, and compromise the network. On the other hand, if the SP controller is compromised, then the entire network is at risk. In this case, a malicious user with access to the main controller can execute any type of requests to the OEM controllers and compromise the optical network. This can be seen in Figure 1.7. In this example, the OEM controllers 1 and 2 receive a flood of requests and execute them in the optical network. This can put the OEM controllers unavailable to the main controller, causing a Denial-of-Service (DoS) attack. In this situation, the OEM controller will have problems processing normal requests alarms, traffic problems, and other notifications from the optical network will be received with a high delay at the SP controller. The worst case will be the entire unavailability of the OEM controller. Such event can lead to interruption of services in the optical network as the common network orchestrator will not see the failures and as such, will not recover the optical

services.

The above security challenges are the motivation for this work. In order to solve the above problems it is important to ensure that all operations executed in the DP (optical equipment) by the OEM controllers are trusted (the requests from the common network orchestrator should not be compromised) and will not compromise the optical equipment functions. It should be also ensured that the OEM controller is always available, independently of external attacks. This is a challenge, and as such is the main motivation of this work.

1.3 Goals

The migration of legacy optical transport networks to SDN should be done without introducing new security problems. The objective of this work is to identify and solve two particular security problems that can arise from the use of optical network equipment with OEM controllers in an SDN environment.

First, it should be ensured that the OEM controller is always available, and capable of processing requests without significant delays. Second, the integrity of the requests should also be guaranteed.

1.4 Contributions

This work will contribute to improve the security of service provider networks on the process of migration to SDN. This is achieved by designing and implementing a monitoring mechanism (reverse proxy) with well defined policies in the OEM controller to prevent DoS attacks. The use of a firewall will also be included. This solution will help SP, to protect their optical networks and make them more resilient in multivendor scenarios.

The mechanism developed in this thesis will be included in the Coriant OEM solutions and documentation, helping our customers, SPs in securing their infrastructure.

1.5 Document outline

In Chapter 2, we present basic concepts about optical networks. In addition, we make a review of the literature of security problems that affect SDN and how they can affect optical SDNs. In Chapter 3, we present the design and implementation of our security solution. This includes the design of mechanisms to protect the OEM controller against some DoS attacks and

man-in-the-middle attacks. In Chapter 4, we evaluate our solution. We end this thesis in Chapter 5, concluding it and presenting the future work.

Chapter 2

Context and related work

This chapter will start by giving an overview of optical networks. The goal is to understand how these networks work, its main challenges and how SPs typically handle them. This initial part also defines the functional and non functional requirements of these networks. Then, we present a security overview for standard SDN networks. This will include security problems, enhancements and solutions. Finally, we consider the main issues in multi-domain optical SDN environments.

2.1 Overview of optical networks

Nowadays, SPs use optical networks to deliver all type of services to their costumers. These networks rely on fibers operated by optical equipment that include optical interfaces [8]. The SP needs to manage and control these networks in order to: compute new paths (when needed), identify points of failures (normally links that need to be repaired or replaced) through alarm information, analyze performance problems, among many other operations. The network management operations are divided in four sub-areas [8]: configuration management (install, remove optical equipment and adjust their settings); connection management (establish cross connections in the equipments to activate end-to-end services in the network); fault management (alarms on optical equipment to identify signal losses or other problems); performance management (information about the quality of the services in all involved optical ports). All this information is used to manage the optical services that run in the optical network. Typically, the Network Management Systems Network Management System (NMS) centralizes all the information (alarms, performance, connections, etc) for each optical service that is running on the optical network. With this approach, SPs are able to see all

the optical services to quickly identify problems. Unfortunately, this is not simple to achieve in multi-domain scenarios. This is a challenge we try to address with an SDN solution.

The SP also requires optical networks to be resilient [23]. These networks transport large quantities of information, making survivability a critical factor. The main goal is to guarantee availability of optical services. As such, the networks have to be designed to recover optical services automatically when failures occur. As explained in the previous chapter, resilience can be divided into multilayer and multi-domain. The focus of this work will be in multi-domain resilience, since we target the scenario of having an OEM controller in each domain (see Figure 1.5), with all domains being controller by a SP controller.

Automatic recovery is very important to guarantee the Service Level Agreements (SLA) that defines the time the overall optical network can be down (the availability of the network). Another parameter that has to be taken into account is service recovery time upon failure (the time spent to change the optical paths from a path with failures to a new path).

To achieve the desired resilience, a good planing for the network deployment is required. This includes protection for the optical links in different locations. In addition, since the SP uses optical equipment from different vendors, it is necessary to protect their optical networks from equipment failures from every specific vendor. Diversity is key for multi-domain resilience (see Figure 1.5).

In the next subsection we present the evolution of optical networks. Then, we define the main operations of optical equipment.

2.1.1 Evolution of optical networks

Optical networks have evolved significantly in the past few years [28]. The first optical networks used a single wavelength per fiber, and were opaque: they could only transport one signal in each optical channel. Later, a new technology was introduced, capable of transporting several signals (frequencies) over a single fiber. This new technology, Wavelength Division Multiplexing (WDM), offers large transmission capacities to optical fibers. The backbone core network (the network that interconnects the metro networks, see Figure 1.2) is highly based on optical links utilizing the WDM technology. More recently this technology has evolved to the Dense Wavelength Division Multiplexing (DWDM), a scheme that makes better use of spectrum to improve the transmission capacities. These networks use predefined connections between the network nodes and pre-planned add and drop wavelength channels. To understand how this is all set up, it is important to

understand optical cards, and its main functions.

2.1.2 Optical equipment overview

In optical networks, network equipment is composed of several cards. The cards can be divided into filters, amplifiers, transponders and muxponders. The transponders and muxponders are composed of two sides, the client and the line side. The client side is where the initial signal is injected. This signal is then encapsulated in a wavelength to be delivered in optical channel (using any frequency available). The main difference between the transponder and the muxponder is in the relation between the client and line side. The muxponder can aggregate several client signals into one line (see Figure 2.1), whereas the transponder can only aggregate one. As such, with a muxponder it is possible to have several low rate signals as clients and multiplex them into a higher rate in the line, and send it to the optical channel. The line side of the transponder or muxponder can then be dropped by a filter and then amplified by an amplifier card (see Figure 2.2). In this figure we show a add and drop scenario with two degrees. Each degree can be seen as a different direction for the optical channel. First, the line side of the transponder or muxponder is connected to the Optical Multiplexer / Demultiplexer (OMD) (a filter card with the fiber connection to the muxponder or transponder) and then the signal flows to the amplifier card (Optical Add Drop Multiplexer (OADM)). This card connects to a similar card in other location by using the optical channel (an example would be optical channel connection between two large cities). All these cards should work together in the same NE.

Optical networks today have to be dynamic, and can change during both planning phase or operation phase, due to traffic changes or due to link or NE failure. To address this issue, Reconfigurable optical add and drop multiplexing (ROADM) and Wavelength Selective Switching (WSS) technology was added. The use of a WSS and ROADM can be seen in Figure 2.3. It allows wavelength reassignment without the need for manual intervention, but with the tradeoff of higher node complexity and cost. Basically, with the WSS it is possible to deliver the signal to any available direction in the NE, and that gives the option to create optical services in any direction. The configuration is executed by the operator via software, allowing the reconfiguration, such as, adding new services or changing existing ones when traffic demands change.

Another recent improvement in the optical network that help operators in management and control includes the Flexi-grid. This solution adds more bandwidth to the optical channels, allowing the transport of more bandwidth

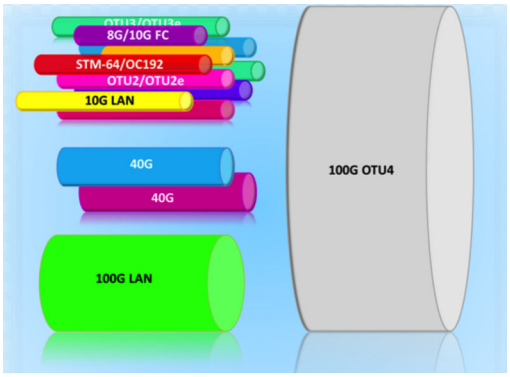

Figure 2.1: Muxponder aggregates several client signals into one line side signal.

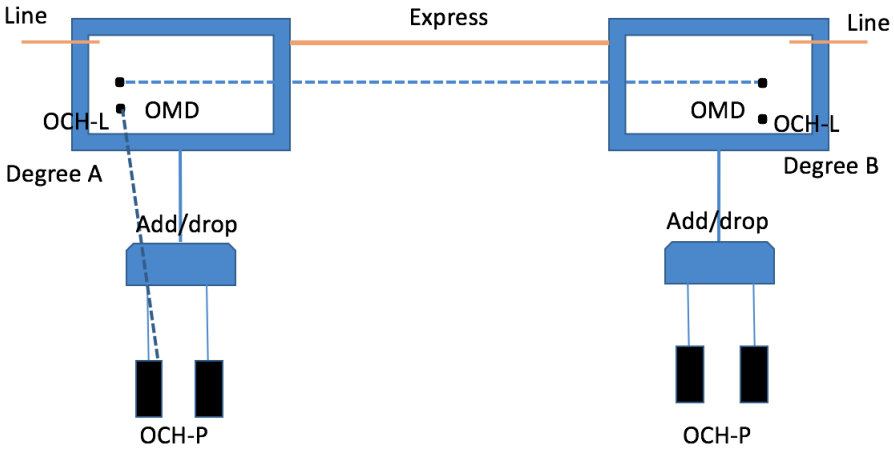

Figure 2.2: Add and drop scenario from a transponder or muxponder to a filter.

in a single optical channel.

Another important technique is the adaptive Rate Modulation, which allows dynamically varying modulation in an errorless manner in order to maximize the throughput under momentary propagation conditions. It also reduces interferences in the network. With this technology, the number of amplifiers can be reduced, consequently reducing network costs.

The Optical Transport Network (OTN) Switch, allows multiple clients to be transparently bundled into uniform containers and sent on a single wavelength. With this technology, clients are decoupled from the transport

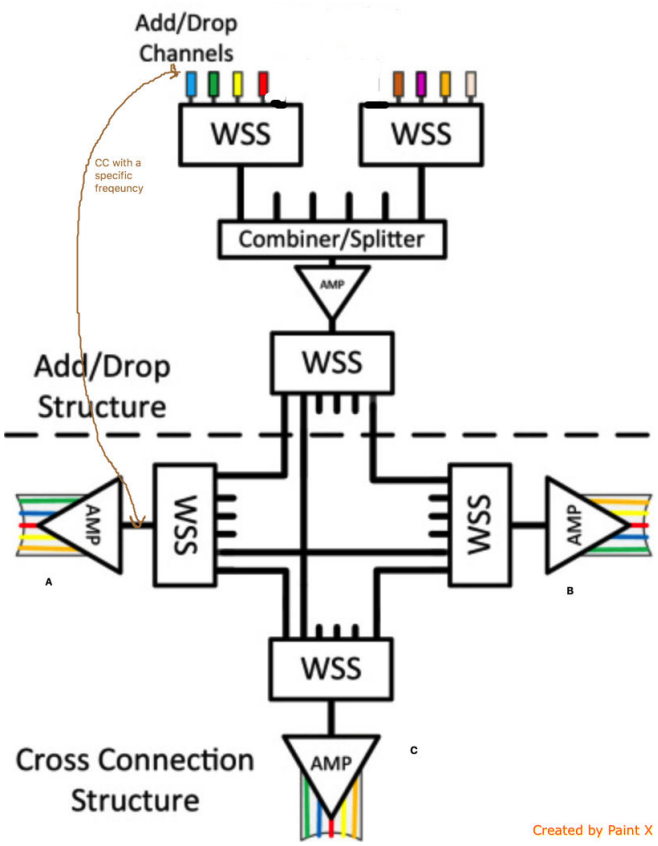

Figure 2.3: ROAMD scenario with WSS

interface, increasing network efficiency.

The new technologies introduced in the past few years have made optical networks more flexible, allowing high degree of control in multi-domain optical environments. As a result, optical networks are changing from static point-to-point systems to mesh topologies with dynamic and diverse wavelengths [28].

2.2 Security overview in Software Defined Networking

The main purpose of security is to preserve confidentiality, integrity and availability of information system resources [27]. Unfortunately, all systems have vulnerabilities which can be exploited by an attacker with the objective to subvert the security policies of the system. These vulnerabilities can

arise from project, implementation, and operation [26]. SDN was not created with security as a priority, and that introduce project vulnerabilities to this paradigm. In addition, the network programability brought up by SDN brings implementation vulnerabilities (due to bad implementation of new software). Finally, if the SDN is not correctly operated, operation vulnerabilities can also appear.

The objective of this section is to give an overview of security in SDN. The focus will be: analysis, enhancements, and solutions. This related work can be used as the basis to improve the security in our scenario, where several OEM controllers are orchestrated by a main SDN controller.

2.2.1 Security analysis in SDN

In this subsection, we give an overview of SDN security. In the literature there are some surveys about security in SDN, [24], [1], [3], and [16]. The security of SDN can be divided into five main components: CP, DP, MP, and communication between them. These components can be seen in Figure 2.4, enumerated from one to five.

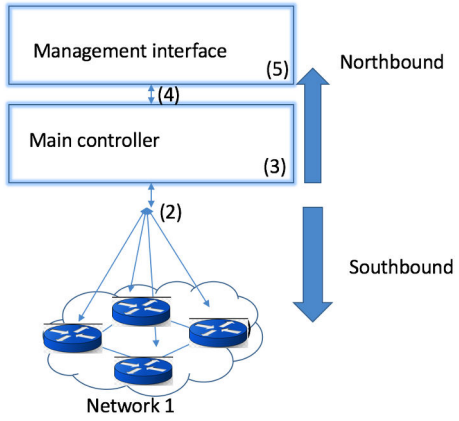

Figure 2.4: Components in SDN.

Several security threats were identified in [16]. First, with forged or faked traffic flows between the NEs an attacker can make a DoS attack to the network by changing flows in the NEs (component 1 in Figure 2.4). Second, vulnerabilities in the NEs can be exploited. For instance, the information retrieved from the NE can be different from the information in the controller. Third, an attack on control plane communication can be used to make DoS attacks or for theft information attacks (man-in-the-middle attacks). Fourth,

attacks to vulnerabilities in the main controller could compromise the whole network. This is the most severe threat in SDN because the controller centralizes the knowledge of the network. Fifth, attacks to the administrative station: these applications are used to access the control plane. If they are compromised, the controller is also compromised, and the whole network is at risk. Sixth, lack of information to make forensics analysis: it's important to have trusted logs about all the operations in the system. Without them it will be impossible to understand the cause of problems that may occur in the network.

To solve the previous problems, the authors of [16] identified the following mechanisms for protection: replication; diversity; self-healing mechanisms; dynamic device association; trust between controllers and the NEs; trust between applications and controllers; security domains; and the use of secure components.

In [13] the authors follow a different approach for the security analysis, focusing on OpenFlow, the standard protocol for SDN. They use the STRIDE method (Spoofing identity; Tampering with data; Repudiation; Information disclosure; Denial of service; Elevation of privilege) [12] with an attack tree approach. They were able to identify the following possible attacks: denial of service against the flow table; hash collision attack on the flow table; observing differences in controller response times to get information (information disclosure), and cache poisoning attacks against the flow table or controller state. In [6], the authors identify new vulnerabilities in OpenFlow that are related with: man-in-the-middle attacks, switch authentication, slow table verification and others.

[2] and [7] addressed the DoS problem. The authors identify several DoS attacks types: Smurf attack, UDP flood attacks, ICMP flood attacks, Syn flood attacks, Teardrop attacks and land attacks. In SDN these attacks can be executed to the network; to the main controller; or to the management Interface.

The smurf attack is a form of DoS attack that can make an entire network unavailable or inoperable. This type of attack explores vulnerabilities in the Internet Protocol (IP) and Internet Control Message Protocols (ICMP) . For this attack, the attacker sends a large amount of ICMP broadcast messages with a spoofed source address (the victim address). By responding to the ICMP messages, the victim will leave the network unavailable.

In the UDP flood attack the attacker sends a large volume of UDP packets to the target system. This will saturate the network, and put legitimate services unavailable.

The ICMP flood attack, explores the use of echo packets to check if the remote host is alive. Basically, the agents send a large volume of ICMP

ECHO REPLY packets to the target victim. The packets request a reply from the victim and by making the reply, the victim will saturate the bandwidth of the network connection. This will make the target system unavailable.

In the SYN flood attack the victims are flooded with half open TCP connections. To establish a TCP connection between a client and a server, the client sends a SYN to the server, and the server responds with a SYN-ACK response message to the client. The connection is only finished when the client responds with the ACK message. Basically, for this attack, the final ACK message is never sent by the client, and a connection stays half open between the client and the server. The server saves the connection state in its structures, but these structures have limited resources. The system may crash or became unavailable for legitimate users.

In the Tear drop attack, the attacker sends long packets, that have to be fragmented. In addition, the attacker sends an invalid offset value into the subsequent fragments. As such, when the packet is reassembled by the victim, if the operating system is not prepared, the system may crash.

In the land attack, the IP address is modified so that the source and destination IPs are the same. This attack works by making the target machine reply to itself continuously.

After this brief security analysis, we will investigate which attacks are valid in a multi-domain optical SDN. This is the topic of the next subsection.

2.2.2 Security analysis in multi-domain optical SDN

To understand the security problems that can affect a multi-domain optical SDN, first it is necessary to identify the differences to standard SDN. Lets begin with its components. In Figure 2.5, we identify the potentially vulnerable components of a multi-domain optical SDN. In this figure, we can see more vulnerable components than in standard SDN. This is due to the addition of OEM controllers between the main controller and the optical network.

In this work, the objective is the protection of the OEM controller. By assuming that the optical network is not compromised, the focus will be the vulnerable components 3 and 4, in Figure 2.5. From [16], an attack to the communication between the main controller and the OEM controller (component 4) can be used for theft information or to modify a legitimate request that will be executed in the network. In this case the integrity of requests will be broken. Another problem is related to DoS attacks. A DoS attack can be executed against the OEM controller (component 3). All the DoS attacks described in the previous subsection will be possible here.

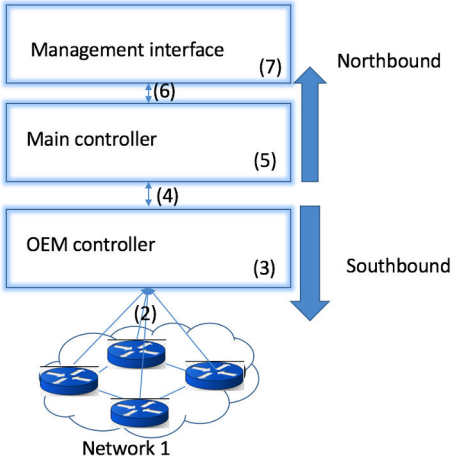

Figure 2.5: Components in multi-domain optical SDN.

In the next subsection we present enhancements and solutions to protect the system from this type of attacks.

2.2.3 Enhancements and security solutions

The problems described in the previous sections (both for standard SDN and for multi-domain optical SDN) can be mitigated through the use of existing security solutions tailored to these settings.

For the DoS attacks several defense mechanisms have been proposed in the literature [2], [7] but, depending on the specific attack, the defense mechanisms may need to be adapted.

To better protect the resources from a DoS attack, it is important to understand what are the main incentives for the attacker. In [30], the authors divide the motivation of the attackers into five main categories:

- **Financial/economical gain:** in this case attacker has a financial gain as the objective. Normally this type of attacks is the most dangerous, and hard to stop. An example for an attack with this objective is simple: imagine that the SP sells to clients a high SLA. In this case, if the optical services stop working for a long time, the client will complain, and the SP may have to pay. In this scenario, the attacker could be a client that wants to receive an indemnity for breaching of the SLA.

- **Revenge:**, in this type of attack, the attacker wants revenge for something that happened. Normally, the attackers have small technical

skills. This type of attacks represents a small threat to the SP.

- **Ideological belief:** In this type of attacks, the attackers are motivated by their ideological beliefs. Some of the attacks can be politically motivated.

- **Intellectual Challenge:** In this type of attacks, the attackers enjoy to experiment and learn how to launch attacks.

- **Cyberwarfare:** In this scenario, the attackers are working for a military or terrorist organization, and they may want to attack critical sections of another country. In this scenario, the target will be the telecommunication network of a country, that is highly dependent of the optical network.

After presenting the main motivations to execute a DoS attack it is important to protect the OEM controller, to guarantee the availability of the optical network. In [31], the authors describe a new algorithm that is inspired in biological systems to implement an Evolving Defence Mechanism (EDM). This algorithm hides network information by implementing a mechanism in the controller that makes: variation of IP addresses; variation of routes; variation of host responses; variation of encryption methods and variation of authentication approaches. By using random network configurations, it is possible to detect on-going attacks and change the network configurations to eliminate security threats according to the security requirements defined for the system. This algorithm can protect the system against several attack types. An example is DoS attacks. When a DoS attack is detected, a variation of the IP address will invalidate the attack (since the IP used for the attack ceases to be valid).

In [30] and [18], the authors describe some generic defense mechanisms that can be used for DoS protection. In [18], the authors divide the defense mechanisms in preventive and reactive.

The **preventive** option has the objective of preventing the attack. The authors divide prevention mechanisms into two groups: Attack prevention and DoS prevention.

Attack prevention uses system security mechanisms and protocol security mechanisms. This can be done, for example, through the use of a firewall. When the firewall detects abnormal traffic, for example a SYN flood attack, the policies defined will block the attack.

The DoS prevention solution, is divided in resource accounting and resource multiplication. In this case, the objective is to have enough resources to enable the victim to endure attack attempts without causing denial the

service to legitimate users. The prevention of a DoS attack is hard, because the attacker can use large scale bot nets to execute the attack, the resources of the victim may not be enough to protect the system.

Another defense mechanism is the reactive approach. The objective of this mechanism is to alleviate the impact of an attack to the victim system. The strategy is to deploy ways to detect attacks through the analysis of resource usage and behavior of the system. In this case, after an attack pattern is detected, the system will react and alleviate the attack. The attacks can be detected through the use of several mechanisms: pattern detection, anomaly detection, or third party detection. With pattern detection, specific attack behaviors are stored in a database. When an attack corresponds to a pattern in the database, the system will react to mitigate it. In the anomaly detection mechanism, the states of the system are periodically compared in order to detect anomalies. The anomaly detection can be standard or trained. The standard operation uses specifications of normal behavior and is based on protocol standards or in sets of rules. In the trained specifications, the normal behavior is specified with thresholds for different parameters. In this case all communication that exceed one or more of these values are considered anomalous. In third party detection, the detection is based on external messages that signals the occurrence of an attack and provide attack characterization.

After the attack is detected, a response strategy to the attack is necessary. To respond to these attacks, the authors of [18] classify reactive mechanisms as agent identification, rate-limiting, filtering and reconfiguration. Agent identification provides information about the machines that are executing the attack. This information will be used to alleviate the impact of the attack. Rate limit imposes a limit on a set of packets that are considered malicious. This type of defense may cause false positives. In filtering mechanisms, after the attack is detected, all the attack stream is filtered. Finally, in a reconfiguration mechanism the topology of the system is reconfigured with either more resources, or the isolation of the attack machines.

The previous mechanisms, together, can represent a good defense to DoS attacks.

2.3 Summary

In this chapter, optical network security problems in SDN were identified, and a number of solutions were presented. This information is the basis for the design of our solution to protect the OEM controller against DoS attacks. That is the topic presented in the next chapter.

Chapter 3

Confidential chapter

Chapter 4

Confidential chapter

Chapter 5

Conclusions

Nowadays, telecommunication systems are critical infrastructures, that have to work 24/7 with little (or no) downtime. Optical network failures, in particular, presents a high cost for the operators (and for society), as a single optical link failure can disrupt an enormous amount of user connections . As such, one of the key requirements of optical networks is *availability*. Optical networks have to be designed with protection mechanisms that allow the recovery of systems after a failure, in a matter of seconds. In multi-domain scenarios, it is very important to synchronize information between network domains, in order to guarantee overall optical network availability. In this scenario, the OEM controller is responsible to abstract the optical network information between the SP controller and the optical equipment. As a consequence, the availability of the OEM controller is a critical point. In this work we have shown that the protection of the OEM controller against DoS attacks is possible.

Our solution to mitigate DoS attacks is composed of two techniques: reverse proxy and firewall. The reverse proxy is used to control the traffic flow in the OEM controller, and the firewall is used to protect the system against some known (D)DoS attacks. The evaluation show that both approaches together represent a good defense agains (D)DoS attacks, and as such guarantee availability. The use of secure communications between the OEM controller and the SP controller is important to protect the integrity of the requests.

Our proposed solution is now being deployed with the installation of Coriant OEM controller. The techniques defined in this work should be added to Nginx configuration, and the documentation be updated with an explanation of the new functionalities. The firewall rules will also be added to the documentation (hardening manual) of the OEM controller. With this work we increase the trust of our system to the SP equipment, influencing

decision makings when choosing SDN products.

5.1 Future Work

For future work, we plan to propose an analysis of a particular type of requests (as these can be malicious) executed be the SP controller. If a malicious user executes malicious operations in the OEM controller, these operations can weaken the optical network (by deleting services for example). As such, if the OEM controller identify that the request is malicious, the request should not be executed in the optical network.

Bibliography

[1] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov. Security in software defined networks: A survey. *Communications Surveys Tutorials, IEEE*, PP(99):1–1, 2015.

[2] Bahaa Qasim M AL-Musawi. Mitigating dos/ddos attacks using iptables. *International Journal of Engineering & Technology*, 12(3), 2012.

[3] S.T. Ali, V. Sivaraman, A. Radford, and S. Jha. A survey of securing networks using software defined networking. *Reliability, IEEE Transactions on*, 64(3):1086–1097, Sept 2015.

[4] B. Belter, A. Binczewski, K. Dombek, A. Juszczyk, L. Ogrodowczyk, D. Parniewicz, M. Stroinski, and I. Olszewski. Programmable abstraction of datapath. In *Software Defined Networks (EWSDN), 2014 Third European Workshop on*, pages 7–12, Sept 2014.

[5] B. Belter, D. Parniewicz, L. Ogrodowczyk, A. Binczewski, M. Stroinski, V. Fuentes, J. Matias, M. Huarte, and E. Jacob. Hardware abstraction layer as an sdn-enabler for non-openflow network equipment. In *Software Defined Networks (EWSDN), 2014 Third European Workshop on*, pages 117–118, Sept 2014.

[6] Kevin Benton, L. Jean Camp, and Chris Small. Openflow vulnerability assessment. In *Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking*, HotSDN '13, pages 151–152, New York, NY, USA, 2013. ACM.

[7] Koushik Chatterjee. Design and development of a framework to mitigate dos/ddos attacks using iptables firewall. *International Journal of Computer Science and Telecommunications*, 4(3):67–72, 2013.

[8] R.D. Doverspike and J. Yates. Optical network management and control. *Proceedings of the IEEE*, 100(5):1092–1104, May 2012.

[9] China Telecom Dr. Yiran Ma. *Perspectives of Beyond 100G*. OFC, 2014.

[10] Gazettabyte. *Verizon readies its metro for next-generation P-OTS*. OFC, 2014.

[11] S. Gringeri, N. Bitar, and T.J. Xia. Extending software defined network principles to include optical transport. *Communications Magazine, IEEE*, 51(3):32–40, March 2013.

[12] Shawn Hernan, Scott Lambert, Tomasz Ostwald, and Adam Shostack. Uncover security design flaws using the STRIDE approach. *MSDN Magazine*, November 2006.

[13] R. Kloti, V. Kotronis, and P. Smith. Openflow: A security analysis. In *Network Protocols (ICNP), 2013 21st IEEE International Conference on*, pages 1–6, Oct 2013.

[14] Teemu Koponen, Martin Casado, Natasha Gude, Jeremy Stribling, Leon Poutievski, Min Zhu, Rajiv Ramanathan, Yuichiro Iwata, Hiroaki Inoue, Takayuki Hama, and Scott Shenker. Onix: A distributed control platform for large-scale production networks. In *Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation*, OSDI'10, pages 351–364, Berkeley, CA, USA, 2010. USENIX Association.

[15] D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig. Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, 103(1):14–76, Jan 2015.

[16] Diego Kreutz, Fernando M.V. Ramos, and Paulo Verissimo. Towards secure and dependable software-defined networks. In *Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking*, HotSDN '13, pages 55–60, New York, NY, USA, 2013. ACM.

[17] E. Mannie. Generalized multi-protocol label switching (gmpls) architecture. RFC 3945, RFC Editor, October 2004.

[18] Jelena Mirkovic and Peter Reiher. A taxonomy of ddos attack and ddos defense mechanisms. *ACM SIGCOMM Computer Communication Review*, 34(2):39–53, 2004.

[19] PMC (Nasdaq:PMCS). *Benefits of OTN in Transport SDN*, pmc-2150738 edition, May 2015.

[20] Damian Parniewicz, Roberto Doriguzzi Corin, Lukasz Ogrodowczyk, Mehdi Rashidi Fard, Jon Matias, Matteo Gerola, Victor Fuentes, Umar Toseef, Adel Zaalouk, Bartosz Belter, Eduardo Jacob, and Kostas Pentikousis. Design and implementation of an openflow hardware abstraction layer. In *Proceedings of the 2014 ACM SIGCOMM Workshop on Distributed Cloud Computing*, DCC '14, pages 71–76, New York, NY, USA, 2014. ACM.

[21] Kumar N. Sivarajan Rajiv Ramaswami and Galen H. Sasaki. *Optical Networks A pratical Perspective*. Morgan Kaufman, third edition edition, 2010.

[22] Victor Lopez Ricard Vilalta. *Multi-technology and Multi-domain Network Orchestration Use Case*. CTTC, ONF, Telefonica.

[23] D.A. Schupke. Multilayer and multidomain resilience in optical networks. *Proceedings of the IEEE*, 100(5):1140–1148, May 2012.

[24] S. Scott-Hayward, G. O'Callaghan, and S. Sezer. Sdn security: A survey. In *Future Networks and Services (SDN4FNS), 2013 IEEE SDN for*, pages 1–7, Nov 2013.

[25] S. Sezer, S. Scott-Hayward, P.K. Chouhan, B. Fraser, D. Lake, J. Finnegan, N. Viljoen, M. Miller, and N. Rao. Are we ready for sdn? implementation challenges for software-defined networks. *Communications Magazine, IEEE*, 51(7):36–43, July 2013.

[26] Miguel Pupo Correia / Paulo Jorge Sousa. *Segurança no Software*. FCA editores, Setembro 2010.

[27] William Stallings. *Computer Security, Principles as Practice*. Pearson, 2012.

[28] Ioannis Tomkos, Biswanath Mukherjee, Steven K. Korotky, Rodney S. Tucker, and Leda Lunardi. The evolution of optical networking. *Proceedings of the IEEE*, 100(5):1017–1022, 5 2012.

[29] China Mobile Weiqiang Cheng. *Use-cases for Packet Transport Network*. IETF, July 2014.

[30] S. T. Zargar, J. Joshi, and D. Tipper. A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks. *IEEE Communications Surveys Tutorials*, 15(4):2046–2069, Fourth 2013.

[31] Haifeng Zhou, Chunming Wu, Ming Jiang, Boyang Zhou, Wen Gao, Tingting Pan, and Min Huang. Evolving defense mechanism for future network security. *Communications Magazine, IEEE*, 53(4):45–51, April 2015.